Hak cipta dan penggunaan kembali:

Lisensi ini mengizinkan setiap orang untuk menggubah, memperbaiki, dan membuat ciptaan turunan bukan untuk kepentingan komersial, selama anda mencantumkan nama penulis dan melisensikan ciptaan turunan dengan syarat yang serupa dengan ciptaan asli.

Copyright and reuse:

This license lets you remix, tweak, and build upon work non-commercially, as long as you credit the origin creator and license it on your new creations under the identical terms.

Team project ©2017
Dony Pratidana S. Hum | Bima Agus Setyawan S. IIP

BAB I

PENDAHULUAN

Latar Belakang

1.1. Cyber-Security telah menjadi salah satu elemen penting dalam sebuah sistem yang terhubung pada jaringan. Bahkan cyber-security telah menjadi bidang yang dikembangkan dikarenakan meningkatnya aktifitas kri*min*al cyber di dunia maya dan munculnya berbagai teknik eksploitasi baru. Salah satu teknik serangan yang populer merupakan *Denial-Of-Service* yang telah menjadi masalah bagi perusahaan yang memberikan layanan berbasis internet.

Beberapa kasus *DDoS* telah dialami oleh perusahaan bernama Dyn, sebuah perusahaan yang mengatur domain website dan mengatur rute lalu lintas internet, yang diserang dengan teknik *DDoS* menggunakan *Mirai botnet* pada tahun 2016. Serangan ini mengakibatkan situs tertkenal seperti Twitter, HSBC, Github, Spotify, Reddit dan Netflix tidak dapat diakses oleh konsumen [1]. Kasus ini menyebabkan Dyn untuk kehilangan 14,000 domain konsumen dari sample sebanyak 178,000 domain [2]. Teknik penyerangan yang digunakan untuk menyerang DNS Server merupakan kombinasi penyerangan pada *Application Layer* dan *Transport Layer* dengan mengirimkan *SYN Flood* pada port DNS Server [3].

Beberapa solusi yang telah ditemukan untuk dapat mengatasi masalah serangan *DDoS*, salah satunya merupakan metode pendeteksian berdasarkan dari kejadian anomali pendekatan berbasis *Machine Learning* untuk mendeteksi kejadian anomali pada jaringan komputer. Metode *Machine*

Learning yang cukup populer untuk pendeteksian anomali adalah *Naïve Bayes Classifier* seperti yang digunakan pada riset berjudul "*A System Approach to Network Modeling for DDoS Detection using a Naìve Bayesian Classifier*" [4] dan "*Detection of DoS/DDoS attack against HTTP Servers Using Naive Bayesian*" [5]. Riset tersebut menggunakan metode *n packet count windowing*, yaitu sebuah metode yang menyimpan paket yang diterima sebanyak *n* untuk dapat dianalisa dan menghasilkan sebuah prediksi oleh sistem.

Kedua riset tersebut tidak menyebutkan bahwa sistem yang dirancang menggunakan struktur data yang efisien untuk proses penghitungan dan pengumpulan data. Namun bila sistem menggunakan struktur data linear, maka sistem akan menghadapi masalah kecepatan prediksi saat *distinct flow* pada lalu lintas jaringan sangat bervariasi. Sehingga membutuhkan waktu yang lebih banyak untuk mendapatkan nilai *count* untuk prediksi setiap *distinct flow* yang baru.

Count-Min Sketch [6] merupakan sebuah struktur data probabilistik berbasis *sketch* dan merupakan implementasi lanjutan dari struktur data *Bloom Filter* [7]. *Count-Min Sketch* telah diimplementasikan pada berbagai macam sistem, salah satunya diimplementasikan pada sistem berbasis NetFPGA pada journal riset "*Implementing On-line Sketch-Based Change Detection on a NetFPGA Platform*" [8] dan sistem yang dirancang mampu memproses lalu lintas jaringan dengan kecepatan 4Gbps dengan akurasi sebesar 97.61% [8].

Maka dari itu penelitian ini mengukur kecepatan dan akurasi prediksi terjadinya serangan *DDoS SYN Flood* dengan menggunakan struktur data

Count-Min Sketch pada *Anomaly Detection System* berbasis *Naïve bayes* dan membandingkannya kecepatan dan akurasinnya dengan penggunaan struktur data linear.

1.2. Rumusan Masalah

Berdasarkan dari latar belakang, masalah yang dapat dirumuskan adalah bagaimana implementasi *Count-Min Sketch* pada *Anomaly Detection System* berbasis *Naive Bayes* mempengaruhi akurasi dan kecepatan prediksi penyerangan *DDoS SYN Flood* jika dibandingkan dengan penggunaan struktur data linear.

1.3. Batasan Masalah

Penelitian lebih memfokuskan pada pendeteksian penyerangan DDoS dengan teknik *SYN Flood*.

1.4. Tujuan Penelitian

Penelitian ini mempunyai tujuan berikut :

- Mengimplementasikan struktur data *Count-Min Sketch* pada *Anomaly Detection System* berbasis *Naïve Bayes*.
- Membuktikan bahwa struktur data *Count-Min Sketch* dapat menambahkan kecepatan dan akurasi *Anomaly Detection System* berbasis *Naïve Bayes* dan *Linked-List*.

1.5. Manfaat Penelitian

Hasil penelitian implementasi *Count-Min Sketch* pada *Anomaly Detection System* berbasis Naïve Bayes diharapkan dapat memberikan wawasan dan dapat menjadi sebuah acuan terhadap pihak yang ingin

mengembangkan *Anomaly Detection System* berbasis *Naïve Bayes* dan *Count-Min Sketch* lebih lanjut.

UMN
UNIVERSITAS
MULTIMEDIA
NUSANTARA